

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

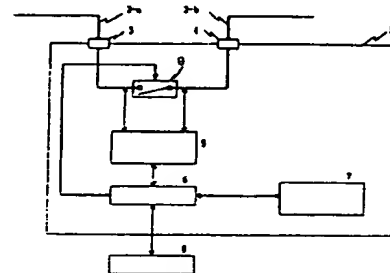
**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

(54) MUTUAL CONNECTION CONTROLLER

(11) 5-219058 (A) (43) 27.8.1993 (19) JP
(21) Appl. No. 4-16617 (22) 31.1.1992
(71) SANYO ELECTRIC CO LTD (72) TSUZUKI KONISHI
(51) Int. Cl⁵. H04L12/28, H04Q9/00

PURPOSE: To automatically set the address of an equipment and to specify the set address of the equipment by a user.

CONSTITUTION: Plural equipments are cascaded by two-way control buses 2-1 and 2-b as a common communication transmission line and then send and receive information to and from each other through the two-way control buses 2-a and 2-b; and the equipments connected to the two-way control buses 2-a and 2-b has their equipment addresses automatically set in the order of the cascade connections of the two-way buses by providing a rewritable storage part 7 for storing only their own equipment addresses and a switch 9 which disconnects two connectors 3 and 4 of the two-way control buses 2-a and 2-b required for the cascade connections in the system.



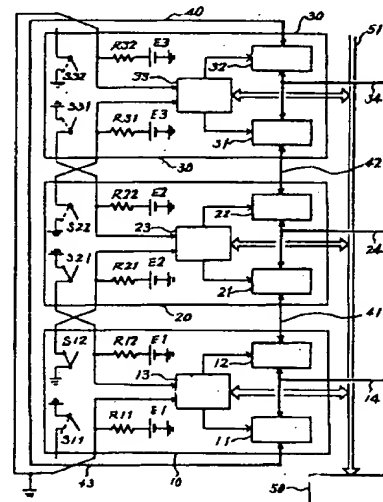
5: control bus transmission and reception part, 6: process part, 8: equipment

(54) UNIT PACKAGE CONNECTION SYSTEM FOR COMMUNICATION CHANNEL

(11) 5-219059 (A) (43) 27.8.1993 (19) JP
(21) Appl. No. 4-20798 (22) 6.2.1992
(71) NEC CORP (72) HARUHIKO KINASHI
(51) Int. Cl⁵. H04L12/28, H04B1/74

PURPOSE: To enable device units except a halfway unit which is disabled to make a communication to make a communication if the halfway device unit is disabled to make the communication in a system wherein the device units equipped with packages are connected in series by a connection line to have a mutual communication.

CONSTITUTION: The packages 10, 20, and 30 can make the communication through connection channels 41 and 42, and a communication channel 40 (by-pass channel 43) which directly connects the packages 10 and 30 is further provided. This communication channel 40 is not used when the system is normal, but if, for example, the package 20 is extracted to disable the packages 10 and 30 to make the communication through the connection channels 41 and 42, the communication channel 40 functions to enable the communication between the packages.



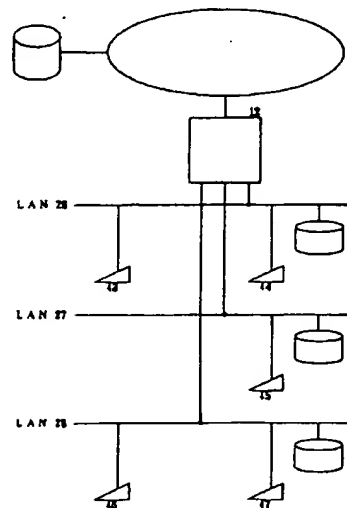
11, 12, 21, 22, 31, & 32: gate part, 13, 23, & 33: control part, 14, 24, & 34: distributor, 50: central control part, 51: controller

(54) INTER-LAN CONNECTING DEVICE

(11) 5-219060 (A) (43) 27.8.1993 (19) JP
(21) Appl. No. 4-40728 (22) 31.1.1992
(71) MATSUSHITA ELECTRIC IND CO LTD (72) MAKOTO MIWA(4)
(51) Int. Cl⁵. H04L12/28

PURPOSE: To provide the inter-LAN connecting device for realizing such filtering of a packet as traffic from a specific terminal is not allowed to flow into other LAN than a designated LAN at a high speed, and also, without being accompanied with an increase of a hardware.

CONSTITUTION: In the inter-LAN connecting device 12 for connecting plural LANs 25-28 by a data link layer or a network layer, this device is provided with a filtering means for filtering a packet by an address of a transmitting origin of a received packet. An associative memory of the inter-LAN connecting device is provided with a storage area of a filtering table with the transmitting origin address and a storage area of a filtering table with a destination address, and a ratio of each area is distributed in accordance with a ratio of the number of entries of each filtering table. As for the packet whose transmitting origin is a specific terminal, its sending destination is limited by this filtering means.



33: data base server, 34, 35, 36: data base server

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平5-219060

(43)公開日 平成5年(1993)8月27日

(51)Int.Cl.⁵

H 0 4 L 12/28

識別記号

庁内整理番号

F I

技術表示箇所

8948-5K

H 0 4 L 11/ 00

3 1 0 C

審査請求 未請求 請求項の数3(全 5 頁)

(21)出願番号 特願平4-40728

(22)出願日 平成4年(1992)1月31日

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 三輪 真

神奈川県横浜市港北区綱島東四丁目3番1

号 松下通信工業株式会社内

(72)発明者 二之部 直久

神奈川県横浜市港北区綱島東四丁目3番1

号 松下通信工業株式会社内

(72)発明者 鬼頭 勉

神奈川県横浜市港北区綱島東四丁目3番1

号 松下通信工業株式会社内

(74)代理人 弁理士 役 昌明 (外1名)

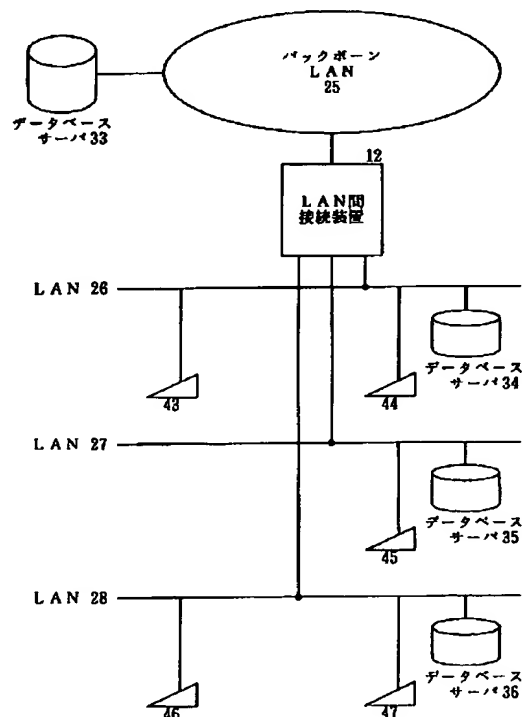
最終頁に続く

(54)【発明の名称】 LAN間接続装置

(57)【要約】

【目的】 特定の端末からのトラヒックを指定したLAN以外に流入させないようなパケットのフィルタリングを高速に、且つ、ハードウェアの増加を伴わずに、実現するLAN間接続装置を提供する。

【構成】 複数のLAN25~28をデータリンク層またはネットワーク層で接続するLAN間接続装置12において、受信したパケットの送信元のアドレスによってパケットをフィルタリングするフィルタリング手段を設ける。LAN間接続装置の連想メモリには、送信元アドレスによるフィルタリング・テーブルの記憶領域と宛先アドレスによるフィルタリング・テーブルの記憶領域とを設け、各領域の割合を各フィルタリング・テーブルのエントリー数の比に応じて配分する。特定の端末を送信元とするパケットは、このフィルタリング手段によって送り先が限定される。



【特許請求の範囲】

【請求項1】 複数のLANをデータリンク層またはネットワーク層で接続するLAN間接続装置において、受信したパケットの送信元のアドレスによって前記パケットをフィルタリングするパケット・フィルタリング手段を設けたことを特徴とするLAN間接続装置。

【請求項2】 宛先アドレスによって前記パケットをフィルタリングするパケット・フィルタリング手段を併せて具備することを特徴とする請求項1に記載のLAN間接続装置。

【請求項3】 送信元アドレスによるフィルタリング・テーブルの記憶領域と宛先アドレスによるフィルタリング・テーブルの記憶領域とを具備する連想メモリを備え、前記各記憶領域の占める割合を前記各フィルタリング・テーブルのエントリー数の比に応じて配分したことを特徴とする請求項2に記載のLAN間接続装置。

【発明の詳細な説明】**【0001】**

【産業上の利用分野】 本発明は、複数のLANを接続してネットワークを構成するLAN間接続装置に関し、特に、LAN間のデータ伝送におけるセキュリティ機能を持たせたものである。

【0002】

【従来の技術】 LAN間接続装置は、図4に示すように、端末41、42やデータベース・サーバ31、32等の機器類を接続した各種のLAN20、21、22、23、24を繋いでネットワークを構成している。図4において、LAN間接続装置10は、バックボーン（幹線）LAN20と支線LAN21、22および23とを接続し、また、LAN間接続装置11は、バックボーンLAN20と支線LAN24との間を

接続している。
【0003】 LAN間接続装置の内部には、図3に示すように、各LANとのインターフェースをとるLANインタフェース61、62、63、64と、各LANから受信したパケットを一時的に格納する共通メモリ2と、フィルタリング・テーブルを記憶する内容検索メモリ（連想メモリ：CAM）3と、CPU、ROM、RAMおよび周辺回路からなる制御部1と、各LANインタフェース61～64、制御部1および共有メモリ2間的高速データ転送を行なうデータ・バス5と、制御部1および連想メモリ3間のデータ転送を行なうローカル・バス4とを備えている。

【0004】 LAN間接続装置11は、ある特定のプロトコル（例えば、TCP/IP）のパケットに対しては、ネットワーク層での接続を提供し（すなわち、ルータとして動作し）、その他のプロトコルのパケットに対してはデータリンク層での接続を提供する（すなわち、ブリッジとして動作する）。

【0005】 各LANインタフェース61～64から受信したパケットは、一旦、共有メモリ2に転送して記憶さ

れ、その後、パケットに含まれるネットワーク層あるいはデータリンク層アドレス（MACアドレス）に従って、該当するLANインタフェース61～64から送信される。

【0006】 内容検索メモリ3には、宛先MACアドレスに対して送信すべきLANの物理的番号を定めたフィルタリング・テーブルが記憶されている。このフィルタリング・テーブルは、図5に例示するように、宛先MACアドレスに対応して、パケットを受信する受信ポート（LAN）毎の送信ポート（LAN）の組合せについて規定している。この例では、LAN間接続装置が、接続する3つのLANの内の第2のLAN（ポート2）から、MACアドレスX宛のパケットを受信した場合に、ポート1に送信（中継）し、ポート3には送信しないこと、また、第3のLAN（ポート3）からそのパケットを受信した場合には、ポート1およびポート2から送信すること等が規定されている。

【0007】 制御部1では、LAN間接続装置からのパケットの送信が、この内容検索メモリ3で設定したフィルタリング・テーブルにしたがって処理されるように、装置の制御を行なっている。また、この処理を高速で実行できるように、アドレスの一致の判断には連想メモリが用いられている。

【0008】 この従来のLAN間接続装置におけるパケット・フィルタリングは、ネットワーク間の不要なトラヒックの増加を抑制し、また、パケットの送信先を特定してセキュリティを確保する機能を果している。

【0009】

【発明が解決しようとする課題】 しかし、従来のLAN間接続装置では、宛先アドレスによってフィルタリングを行なっているため、ある端末からのトラヒックを別のLANに流入させないようなフィルタリングを行なうことができない。例えば、図4のバックボーンLAN20上のデータベース・サーバ31に対して、支線LAN22の特定の端末（データベース・サーバ32）からはアクセスできるが、一般の端末42からはアクセスできないような設定とすることができず、そのような形でのセキュリティの実現を図ることができなかった。

【0010】 本発明は、このような従来の問題点を解決するものであり、特定の端末からのトラヒックを指定したLAN以外に流入させないようなパケットのフィルタリングを高速に、且つ、ハードウェアの増加を伴わずに、実現できるLAN間接続装置を提供することを目的としている。

【0011】

【課題を解決するための手段】 そこで、本発明では、複数のLANをデータリンク層またはネットワーク層で接続するLAN間接続装置において、受信したパケットの送信元のアドレスによってパケットをフィルタリングするフィルタリング手段を設けている。

【0012】また、宛先アドレスによってパケットをフィルタリングするフィルタリング手段と併せて前記送信元アドレスによるフィルタリング手段を設けている。

【0013】さらに、LAN間接続装置に、送信元アドレスによるフィルタリング・テーブルの記憶領域と宛先アドレスによるフィルタリング・テーブルの記憶領域とを具備する連想メモリを設け、各記憶領域の占める割合を各フィルタリング・テーブルのエントリー数の比に応じて配分している。

【0014】

【作用】そのため、特定の端末を送信元とするパケットの送り先のLANをフィルタリング手段によって限定することができる。また、このフィルタリングに使用するテーブルを、宛先アドレスによるフィルタリング・テーブルと共に連想メモリに記憶させることにより、ハードウェアの増設を必要としない。

【0015】

【実施例】本発明の実施例におけるLAN間接続装置は、図1に示すように、データベース・サーバ33を備えたバックボーンLAN25と、データベース・サーバ34、35、36および一般端末43、44、45、46、47を備えた複数の支線LAN26、27、28とを接続してネットワークを形成している。ここで、一般端末43以外の端末33～36、44～47は、TCP/IPプロトコルを実装しているものとする。

【0016】LAN間接続装置12の内部構成は、図3に示すものと変わらない。ただ、内容検索メモリ（連想メモリ）3には、図2のメモリ・マップに示すように、MACアドレスによるフィルタリング・テーブルを格納するMACアドレス・フィルタリング領域52の外に、ネットワーク層（IP）アドレスによるフィルタリング・テーブルを格納するIPアドレス・フィルタリング領域53が設けられている。

【0017】このIPアドレス・フィルタリング領域53のフィルタリング・テーブルは、送信元IPアドレスによってパケット・フィルタリングを行なうためのテーブルである。

【0018】図1のネットワークにおいて、バックボーンLAN25のデータベース・サーバ33に対するアクセスは、各支線LAN26～28のデータベース・サーバ34、35、36からは可能であるが、一般端末43～47からはアクセスできないものとする。但し、一般端末44～47は、端末43を除いて、各々の支線LAN上のデータベース・サーバ34～36にはアクセスすることができる。

【0019】このとき、LAN間接続装置12の連想メモリ3のIPアドレス・フィルタリング・テーブルには、送信元のIPアドレスに対応して、受信ポートと送信ポートとの関係を次の（1）～（4）のようにエントリーする。このエントリー以外のIPアドレスに対しては、全てフィルタリングされる。

【0020】（1）送信元のIPアドレスがデータベース・サーバ34のときは、LAN26のポートからLAN25のポートへの送信のみTrue、（2）送信元のIPアドレスがデータベース・サーバ35のときは、LAN27のポートからLAN25のポートへの送信のみTrue、（3）送信元のIPアドレスがデータベース・サーバ36のときは、LAN28のポートからLAN25のポートへの送信のみTrue、（4）送信元のIPアドレスがデータベース・サーバ33のときは、LAN25のポートから他の全てのLAN26～28のポートへの送信がTrue。

【0021】LAN間接続装置の制御部1では、パケットを受信すると、そこに含まれる送信元のIPアドレスから、IPアドレス・フィルタリング・テーブルに基づいてパケットの送信先を決め、該当するLANに送信する。その結果、データベース・サーバ33に対しては、データベース・サーバ34、35、36からのアクセスのみが可能となり、セキュリティが保持される。

【0022】連想メモリ3では、システム固有領域51以外の領域がMACアドレス・フィルタリング領域52とIPアドレス・フィルタリング領域53とに分割されるが、この領域分割は、装置の初期化時に定められる。

【0023】各領域の占める割合は、MACアドレス・フィルタリングのエントリー数とIPアドレス・フィルタリングのエントリー数との比に応じて設定される。

【0024】このエントリー数の比は、結局、プロトコル別の端末数の分布に依存することになり、図1の例のように、大部分の端末が共通してTCP/IPプロトコルを実装し、それ以外のプロトコルの端末43の台数が少ないネットワークでは、ブリッジ動作をするパケットの発生量が少ないため、MACアドレス・フィルタリング領域52の占める割合は小さく、大部分がIPアドレス・フィルタリング領域53として用いられる。

【0025】このように、連想メモリをMACアドレス・フィルタリング・テーブルとIPアドレス・フィルタリング・テーブルとに共用し、その領域の比率を端末の状況に応じて決めることにより、ハードウェア資源の有効利用が図れる。また、IPアドレス・フィルタリングを連想メモリで実現しているため、高速処理が可能となる。

【0026】

【発明の効果】以上の実施例に基づく説明から明らかなように、本発明のLAN間接続装置では、パケットの送信元のアドレスに基づいてフィルタリングすることにより、ネットワークの不要なトラフィックを制限し、セキュリティの向上を図ることができる。また、そのフィルタリングの動作を高速に処理することができ、さらに、従来のLAN間接続装置と同程度のハードウェアによって、このフィルタリングを実行することができる。

【図面の簡単な説明】

【図1】本発明のLAN間接続装置を用いた実施例にお

けるネットワーク構成図、

【図2】前記LAN間接続装置の連想メモリのメモリ・マップ概念図、

【図3】LAN間接続装置の内部構成図、

【図4】従来のLAN間接続装置を用いたネットワーク構成図、

【図5】従来のフィルタリング・テーブルを示す図である。

【符号の説明】

- 1 制御部
- 2 共有メモリ
- 3 内容検索メモリ（連想メモリ）

* 4 ローカル・バス

5 データ・バス

10~12 LAN間接続装置

20、25 バックボーンLAN

21~24、26~28 支線LAN

31~36 データベース・サーバ

41~47 一般端末

51 システム固有領域

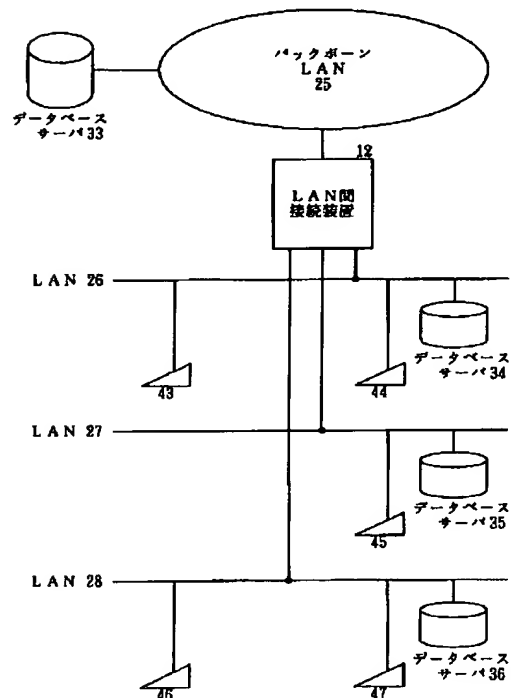
52 MACアドレス・フィルタリング領域

10 53 IPアドレス・フィルタリング領域

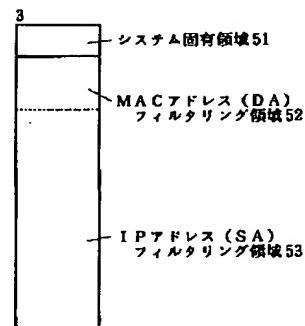
61~64 LANインタフェース

*

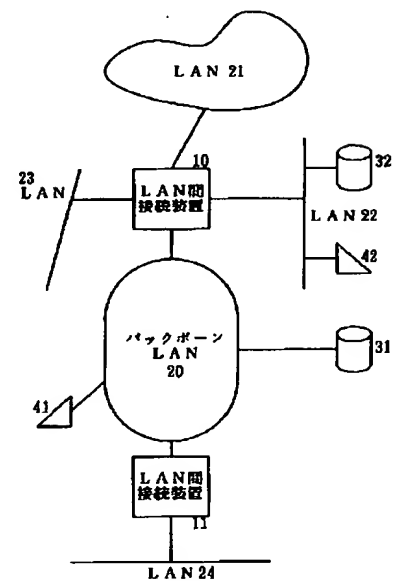
【図1】



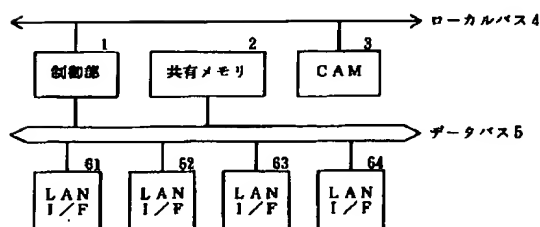
【図2】



【図4】



【図3】



【図5】

MACアドレス	ポートマップ																				
MACアドレス X	<table><tr><td colspan="4">バケット送信ポート番号</td></tr><tr><td>バケット</td><td>1</td><td>2</td><td>3</td></tr><tr><td>受信ポ</td><td>1 False</td><td>False</td><td>True</td></tr><tr><td>ート番</td><td>2 True</td><td>False</td><td>False</td></tr><tr><td>号</td><td>3 True</td><td>True</td><td>False</td></tr></table>	バケット送信ポート番号				バケット	1	2	3	受信ポ	1 False	False	True	ート番	2 True	False	False	号	3 True	True	False
バケット送信ポート番号																					
バケット	1	2	3																		
受信ポ	1 False	False	True																		
ート番	2 True	False	False																		
号	3 True	True	False																		

フロントページの続き

(72)発明者 武佐 睦
神奈川県横浜市港北区綱島東四丁目3番1
号 松下通信工業株式会社内

(72)発明者 森 孝志
神奈川県横浜市港北区綱島東四丁目3番1
号 松下通信工業株式会社内